PATENT COOPERATION TREATY

To:

YOU ME PATENT AND LAW FIRM
Seolim Bldg., 649-10,
Yoksam-dong, Kangnam-ku,
Seoul 135-080
Republic of Korea

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	29 July 2005 (29.07.2005)
Applicant's or agent's file reference: OPP040038KR	FOR FURTHER ACTION: See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority Date *(day/month/year)*
PCT/KR 2004/003212	8 December 2004 (08.12.2004)	9 December 2003 (09.12.2003)

International Patent Classification (IPC) or both national classification and IPC
H04N 7/16, H04N 7/173, H04Q 7/22, H04Q 7/38, H04L 29/06

Applicant
ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE

1. This opinion contains indications relating to the following items:

- ☒ Cont. No. I — Basis of the opinion
- ☐ Cont. No. II — Priority
- ☐ Cont. No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Cont. No. IV — Lack of unity of invention
- ☒ Cont. No. V — Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Cont. No. VI — Certain documents cited
- ☐ Cont. No. VII — Certain defects in the international application
- ☐ Cont. No. VIII — Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ AT
Austrian Patent Office
Dresdner Straße 87, A-1200 Vienna

Facsimile No. +43 / 1 / 534 24 / 535

Authorized officer
MESA PASCASIO J.

Telephone No. +43 / 1 / 534 24 / 327

Continuation No. I

Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed.

Continuation No. V

Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims **1-22**	**YES**
	Claims **----**	**NO**
Inventive step (IS)	Claims **----**	**YES**
	Claims **1-22**	**NO**
Industrial applicability (IA)	Claims **1-22**	**YES**
	Claims **----**	**NO**

2. Citations and explanations:

The cited documents of the Search Report are:

D1: IEEE Std. 802.16-2001
D2: US 2003/0078061 A1

Document D1, the standard for a wireless portable Internet system, defines a method of generating and distributing a traffic encryption key to be used for security on a traffic connection so as to encrypt traffic data prior to establishing the traffic connection. According to this method, the subscriber station (SS) and the base station (BS) use PKM-REQ (Privacy Key Management-Request) message and PKM-RSP (Privacy key Management-Response) message so as to generate and distribute a traffic encryption key. Herein, the PKM-REQ message and the PKM-RSP message are related to authentication. Thus, the SS sends a Key Request message, which is an internal message of the PKM-REQ messages, to the BS to request a traffic encryption key from the BS, and the BS sends a responding message to the SS. In detail, the BS sends a Key Reply message to the SS when the refreshment of the traffic encryption key is successful or a Key Reject message to the SS when the refreshment of the traffic encryption key is failed. The traffic encryption key is newly generated and distributed throughout the foregoing method, and the SS and the BS encrypt traffic data for transmission using the traffic encryption key.

Document D2 provides a method and an apparatus for providing only authorized mobile subscribers with a specified commercial broadcasting service in a cellular mobile

communication network. A base station transmits a control signal including a common traffic ciphered key having a specified validation period through a dedicated secure signal channel assigned to a respective authorized subscriber terminal. The base station then enciphers broadcasting data from a broadcasting system with the common traffic ciphered key, for broadcasting through a common traffic broadcasting channel. The base station periodically updates the common traffic ciphered key according to the corresponding validation period. A subscriber terminal obtains the common traffic ciphered key from the control signal received through the dedicated secure signal channel, and deciphers the broadcasting signal with the obtained common traffic ciphered key to obtain therefrom the broadcasting data. The broadcasting data is displayed after a predetermined video signal processing.

Such a method for generating and distributing a traffic encryption key defined by the IEEE 802.16 wireless portable Internet system is confined to the unicast service between the SS and the BS. Therefore, the multicast service and the broadcast service are taken into consideration in the IEEE 802.16 wireless portable Internet system so as to provide extendable and secure services to a large number of subscribers as provided in the present application. Distributing broadcasting data to a number of authorized subscribers is subject matter of D2. Therefore, with the knowledge of D1 and D2 a person skilled in the art is able to extend the standard D1 with the features of D2 in an easy way.

Accordingly, all claims 1 to 22 are new but do not include an inventive step.

Industrial applicability is given.